



**INITIATIVE WITH DRAFT DECREE BY WHICH THE LAW IS ISSUED
FEDERAL FOR THE ETHICAL, SOVEREIGN AND INCLUSIVE DEVELOPMENT OF THE
ARTIFICIAL INTELLIGENCE**

The undersigned, members of the parliamentary group of MORENA and the parliamentary group of the Green Ecologist of Mexico, **Gabriela Georgina Jiménez Godoy, Sergio Carlos Gutiérrez Luna, Eruviel Ávila Villegas, Javier Octavio Herrera Borunda, Leonel Godoy Rangel, Hugo Eric Flores Cervantes, Alfonso Ramírez Cuéllar, Olga María del Carmen Sánchez Cordero, Giselle Yunueen Arellano Ávila, Herminia López Santiago, José Armando Fernández Samaniego, Monica Angelica Alvarez Nemer, Alma Laura Ruiz López, Mónica Herrera Villavicencio, Jesús Irugami Perea Cruz, Jesús Alfonso Ibarra Ramos, Sergio Mayer Bretón, Julieta Kristal Vences Valencia, Guillermo Rafael Santiago Rodríguez, Gloria Sánchez Lopez, Danisa Magdalena Flores Ojeda, Monica Fernandez Cesar, Juan Angel Flores Bustamante, Jose Javier Aguirre Gallardo, Ulises Mejia Haro, Eden Garces Medina, Gilberto Herrera Solórzano, Claudia Garcia Hernandez, Marisela Zuniga Ceron, Francisco Arturo Federico Avila Anaya, Joaquín Zebadúa Alva and Alejandro Carvajal Hidalgo** in the LXVI Legislature of the Honorable Congress of the Union, based on the provisions of Article 71, Section II of the Political Constitution of the United States Mexicans; as well as by articles 6, numeral 1, section I; 77 and 78 of the Regulations of the Chamber of Deputies, submit the following to the consideration of this Honorable Assembly:

Initiative with draft decree issuing the **Federal Law for the Ethical, Sovereign and Inclusive Development of Artificial Intelligence**, as follows:

STATEMENT OF REASONS

Artificial intelligence represents one of the most significant technological advances in contemporary history, with a cross-cutting impact on the economic, social, educational, political, and cultural spheres. Its accelerated expansion is redefining the way we produce goods, provide services, access education, participate in democratic life, and interact in society. The decisions made by



Automated systems are beginning to directly impact the rights, reputation, integrity, and opportunities of millions of people, without any national regulation to protect them clearly, firmly, and fairly.

The absence of a comprehensive legal framework regulating the development, use, oversight, and control of artificial intelligence in Mexico has created a legal vacuum that fosters opacity, widens inequality gaps, favors technological colonization, and exposes the most vulnerable sectors to risks of lack of protection and digital exclusion.

This legislative omission has created an asymmetry between those who concentrate algorithmic power and those who barely understand its effects.

Therefore, this Law was created as a strategic, timely, and deeply ethical response, based on the conviction that the Mexican State has a duty to ensure that technology is not imposed over human dignity, but rather is used as a tool to promote social justice, digital inclusion, equal opportunities, and the country's technological sovereignty.

The purpose of this law is to establish a comprehensive regulatory framework to ensure that the development and implementation of artificial intelligence in Mexico is carried out under the principles of legality, transparency, equity, human oversight, precaution, sustainability, and unrestricted respect for human rights. Its approach is not punitive or restrictive in nature, but rather eminently enabling: it seeks to channel the potential of artificial intelligence toward responsible innovation, economic growth with social justice, and scientific advancement in the service of the public interest and collective well-being.

This legislative initiative proposes a new regulatory paradigm in which artificial intelligence ceases to be a tool for concentrating power and becomes an agent at the service of social justice, human dignity, technological sovereignty, and inclusive and sustainable development.

The Federal Law for the Ethical and Inclusive Development of Artificial Intelligence initiative is designed **not to inhibit innovation, but to enable it responsibly.** To ensure that **progress**



technological development contributes to closing gaps, not deepening them, and that every advance in this area has shared well-being as its goal.

This proposal is based on solid legal principles, the **current constitutional framework, the Mexican State's international commitments, and standards recognized by multilateral organizations such as UNESCO, the OECD, the Council of Europe, and the European Commission,** whose regulatory frameworks have served as a reference for this legislative design.

The proposal is based on a vision that recognizes both the benefits and risks of this technology. On the one hand, it is essential to promote innovation, national talent, open knowledge, and social entrepreneurship in Artificial Intelligence (AI). On the other hand, it is imperative to prevent these technologies from reproducing or deepening structural gaps, discriminating uncontrollably, making decisions without explanation, or generating unacceptable environmental impacts. Faced with these scenarios, the Law proposes a robust, adaptive digital legal architecture with concrete tools for effective regulation.

It is important to note that Mexico is part of the 2030 Agenda, created in 2015. It proposes 169 goals through 17 Sustainable Development Goals. The main objective is to leave no one behind and achieve their full achievement by 2030. Thus, our country maintains a firm commitment to fulfilling this agenda. This law seeks to strengthen SDGs 1, 4, 8, 9, 11, 12, and 17.

Artificial Intelligence, from its application and regulation, has various benefits, which in turn tie in with different points of the Plan

Mexico in points 3, 5, 9, 10, and 11, which was presented by the President of the United Mexican States Claudia Sheinbaum Pardo in

By 2025, the program aims primarily to strengthen the targeting of resources, identify vulnerable populations, optimize social programs, improve employment efficiency, and improve access to financing for SMEs. It also allows for monitoring and reducing the environmental impact of companies, optimizing supply chains, and improving traceability, contributing to corporate environmental sustainability. Furthermore, automation in the industry is being strengthened, supporting the formation of



technicians and professionals and the increase in national content, which is related to numeral 9 of the Mexico Plan.

The text is composed of 29 chapters that address, in a technical and forward-looking manner, the various components of the artificial intelligence ecosystem. These include general provisions and key definitions, the creation of a National AI Council, an innovative risk traffic light system, a progressive regime of rights, duties, and sanctions, and mechanisms for oversight, reparation, and algorithmic justice. It also addresses strategic topics such as the **protection of children and adolescents from harmful content**, strengthened regulation in sectors such as health, territorial planning, justice, and education, **as well as the obligation to guarantee explainability, technical traceability, and the possibility of appeal** against automated decisions.

Special attention deserves the promotion of Mexican talent, scientific training with a gender perspective, the fostering of sovereign innovation networks, and the establishment of regulatory sandboxes as safe environments for technological experimentation under institutional oversight. Furthermore, for the first time, a specific chapter on digital sustainability and environmental impact is included in national legislation to ensure that the growth of the Artificial Intelligence ecosystem does not contradict climate commitments or pass on its ecological costs to vulnerable communities.

No less important is the establishment of a clear and proportional liability regime, with effective sanctions and accessible mechanisms for reporting and redress. Citizens can no longer be left unprotected against opaque systems that decide their lives without offering explanations or avenues for review. **The Law places the individual at the center of all automated processes, requiring meaningful human oversight, enhanced data protection, special measures for vulnerable populations, and the pro-person principle as the guiding principle of legal interpretation.**

With this legislative proposal, Mexico is moving toward democratic governance of artificial intelligence. Not through blind distrust.



Not from uncritical fascination, but from a position of institutional responsibility, commitment to collective well-being, and a strategic vision for the future. This Law aims to consolidate a country where artificial intelligence is fully at the service of life, social justice, environmental sustainability, and technological sovereignty. Where knowledge is a shared good, technological development is based on ethical principles, and algorithmic power is subject to the same democratic, legal, and social limits as any other form of power.

This Law shall be interpreted and applied in accordance with the principle of responsible innovation, understanding that technological development must be promoted provided that it respects human rights, the public interest, and the principles established herein. No provision of this Law may be applied in a manner that constitutes an unjustified barrier to legitimate experimentation, scientific research, or ethical entrepreneurship.

This is a law that doesn't just regulate: it transforms. It doesn't just warn: it builds. It doesn't just react: it proposes. And it does so with the certainty that artificial intelligence can and should be an ally of the people, of open knowledge, of the environment, and of democracy.

For the reasons stated above, we submit to the consideration of the Honorable Congress of the Union, the following:

Decree creating the Federal Law for Ethical and Sovereign Development Inclusive of Artificial Intelligence

SOLE ARTICLE. The Federal Law for the Ethical, Sovereign Development is hereby issued and Inclusive of Artificial Intelligence.

FEDERAL LAW FOR THE ETHICAL, SOVEREIGN AND INCLUSIVE DEVELOPMENT OF THE ARTIFICIAL INTELLIGENCE

CHAPTER I – PURPOSE, NATURE AND SCOPE OF APPLICATION



Article 1. The purpose of this Law is to establish the general regulatory framework for the development, implementation, use, supervision and promotion of artificial intelligence in the United Mexican States, in accordance with the principles of universality, interdependence, indivisibility, and progressiveness of human rights, ensuring an ethical approach and promoting technological sovereignty. This is to ensure that every person enjoys the benefits derived from development and innovation in the field of Artificial Intelligence, in full observance and respect for Human Rights.

Article 2. This Law is of public order, social interest, and general observance throughout the national territory. Its application corresponds to the federal, state, Mexico City, and municipal authorities, within the scope of their respective powers.

Article 3. The provisions of this Law shall apply to all individuals or legal entities, public or private, national or foreign, that develop, use, market, implement, or interact with artificial intelligence systems that operate in national territory, affect Mexican citizens, utilize Mexican infrastructure, or generate legal effects in Mexico.

Article 4. The interpretation of this Law shall be carried out in accordance with the principles of human dignity, human rights, the best interests of children, technological sovereignty, personal data protection, and social equity. In all matters not expressly provided for, the provisions contained in the Political Constitution of the United Mexican States, international treaties to which Mexico is a party, and laws on data protection, cybersecurity, transparency, science and technology, digital rights, and administrative justice shall apply as a supplement.

CHAPTER II – DEFINITIONS

Article 5. For the purposes of this Law, the following definitions shall apply:

- I. **Machine Learning:** Technique by which an Artificial Intelligence system adjusts its behavior based on data



historical or real-time, without the need for explicit reprogramming, improving their performance on specific tasks.

II. Algorithmic Audit: A technical, legal, and ethical process for reviewing artificial intelligence systems, aimed at identifying biases, errors, risks, or regulatory non-compliance, for the purposes of correction, prevention, or accountability.

III. Automated informed consent: a user's free, specific, informed, and unequivocal expression of consent, through digital means, to have their personal data subject to algorithmic processing by an AI system, having been informed of its scope, consequences, and associated rights.

IV. Training Data: Dataset used to develop and calibrate AI systems. The quality, diversity, and representativeness of this data determines the system's performance, fairness, and reliability.

V. Human right to science: Right recognized in section V of article 3 of the Political Constitution of the United Mexican States, as well as in the international treaties to which the Mexican State is a party, which includes access to advances in the humanities, sciences, technologies and innovation, including their use for the benefit of human and social development.

VI. Regulatory Test Environment in AI: A controlled test environment in which companies, institutions, or research centers can develop, experiment, and evaluate artificial intelligence systems under limited real-life conditions, under the supervision of regulatory authorities, to ensure responsible innovation and early detection of risks.

VII. Equity: The AI should not discriminate against any person based on ethnic or national origin, gender, age, disabilities, social status, health conditions, religion,



opinions, sexual preferences, marital status or any other that violates human dignity and aims to nullify or undermine the rights and freedoms of individuals. Equity in AI aims to eradicate the perpetuation of inequalities and ensure that all individuals can

VIII. Algorithmic Impact Assessment (AIA), estimation of the damage that Artificial Intelligence, its processes and its products can cause to the population.

IX. Explainability of Artificial Intelligence: The ability of an Artificial Intelligence system to provide an understandable explanation of the reasons, criteria, and processes by which it generates automated decisions, enabling their traceability, auditing, and understanding by users or affected parties.

X. Algorithmic Governance: Set of norms, principles, processes and institutions intended to supervise, regulate and control the design, operation and effects of algorithmic systems, based on the public interest, transparency and accountability.

XI. Low-Risk Artificial Intelligence: Artificial intelligence systems that do not pose a significant risk to people's fundamental rights, health, or safety. Their use is free and does not require specific regulatory conditions. Examples: basic personal assistants, spam filters, entertainment recommendation engines.

XII. Limited Risk Artificial Intelligence: Systems that involve moderate risk and require minimal transparency measures, such as user notification about interaction with an AI.

Examples: Virtual information assistants, advertising personalization systems, ultra-fake labeling.

XIII. High-Risk Artificial Intelligence: Systems whose use may have a significant impact on human rights, life, health, or public safety. They are subject to strict design, conformity assessment, explainability, and oversight requirements.



Examples: Artificial Intelligence in health, justice, education, public safety, labor recruitment, authorized biometric surveillance.

XIV. Prohibited Artificial Intelligence: Prohibited artificial intelligence shall be understood to mean those systems whose development, training, implementation, use, commercialization, import or export is prohibited because it represents an unacceptable risk to human dignity, fundamental rights, life, public safety, social peace or democratic stability.

Among others, artificial intelligence systems will be considered that:

- a) Use subliminal manipulation techniques or extreme psychological persuasion to alter human behavior without informed consent.
- b) Establish coercive or discriminatory social scoring mechanisms, implemented by public or private entities.
- c) Carry out mass biometric surveillance in public spaces without express judicial authorization and strict institutional control.
- d) Exploit cognitive, emotional or autonomy vulnerabilities of girls, boys, adolescents, the elderly, people with disabilities or people in situations of psychosocial vulnerability.
- e) They are developed for the creation, improvement or use of weapons for the exclusive use of armed forces.
armed, or that facilitate the development of chemical, biological, radiological or nuclear weapons, prohibited by international treaties.
- f) Are intended for the production or dissemination of explosives, toxic agents or substances intended to cause



damage massive to people either estate.

g) Facilitate or instruct on activities linked to terrorism, the commission of cybercrimes, unauthorized hacking of personal data, identity theft, bank account theft, or any form of attack against critical infrastructure systems.

The ban will be applied broadly and preventively, in accordance with the principles of precaution, enhanced protection of human rights, and safeguarding public safety.

XV. Algorithmic Impact: Direct or indirect consequence generated by an Artificial Intelligence system on people, rights, the environment or institutions, derived from its design, implementation, operation or results.

XVI. Artificial Intelligence (AI): A computer, algorithmic, or physical system designed to emulate human capabilities such as learning, reasoning, perception, or decision-making, which can operate autonomously or assisted, and whose results impact people, processes, or environments, both physical and digital.

XVII. Algorithmic Harm Redress: A legal, administrative, or technical mechanism by which people affected by Artificial Intelligence systems can obtain restitution, compensation, or effective corrective measures against unfair, erroneous, or discriminatory automated decisions.

XVIII. National Registry of Artificial Intelligence Systems (RENSIA) is a public, technical database managed by the competent authority, which will contain key information on artificial intelligence systems classified by risk type.

XIX. Algorithmic Risk: Probability that an artificial intelligence system will generate negative consequences—intentional or not—on the physical, mental, patrimonial, reputational or social integrity of a person, group or institution.



- XX. **Algorithmic Bias:** Systematic or unjustified distortion in the results generated by an AI system, caused by flaws in design, training data, or implementation, which disproportionately affect individuals or groups.
- XXI. **Autonomous AI System:** An artificial intelligence system that, once activated, operates without direct human intervention to generate decisions or actions with effects in physical, digital, or legal environments.
- XXII. **Artificial Intelligence System:** A set of algorithms, data models, computational processes, and physical or virtual components designed to receive input data, analyze it using automated techniques, and generate output in the form of decisions, recommendations, predictions, or actions.
- XXIII. **AI Risk Traffic Light System:** A regulatory classification mechanism that groups artificial intelligence systems into risk levels—minimal, limited, high, or prohibited—based on their potential impact on human rights, security, health, the environment, and democratic institutions.
- XXIV. **Meaningful Human Oversight:** Active, deliberate, and empowered human intervention in the design, oversight, or review of an AI system, with the goal of preventing erroneous, unfair, or disproportionate automated decisions.
- XXV. **Transparency.** This principle means that all information relating to artificial intelligence must be comprehensive, clear, and explainable.
- XXVI. **Algorithmic Traceability:** The ability to reconstruct the functioning, reasoning, and internal path of an AI system, from its input data to its output, in order to evaluate its behavior, explain its decisions, or assign responsibility.



XXVII. **Sensitive Sectors:** Those sectors of public or private activity in which the implementation of artificial intelligence systems may have a significant impact on the fundamental rights, security, life, dignity, or equity of individuals. These include, but are not limited to, the health, education, justice, labor, public safety, mobility, urban services, social development, and financial services sectors.

XXVIII. **National Algorithmic Audit Platform (PNA):** A specialized technical body attached to the National AI Council, responsible for conducting automated or semi-automated evaluations of data sets used to train AI models and systems, identifying risks, biases, or differentiated impacts, and issuing technical reports or risk labels.

XXIX.

CHAPTER III – GUIDING PRINCIPLES AND ASSOCIATED RIGHTS

Article 6. The provisions of this Law shall be governed by the following guiding principles:

- I. **Good Administration:** Obliges authorities using artificial intelligence systems to act effectively, efficiently, impartially, legally, rationally, and with respect for human rights, ensuring access to information, justification of decisions, and appeal mechanisms.
- II. **Human Dignity:** Any development, use, or implementation of artificial intelligence must respect, protect, and promote the inherent dignity of all people. Technology should never be used to diminish, manipulate, or replace the value of the human condition.
- III. **Necessity:** The use of artificial intelligence technologies must respond to a legitimate, specific and justified purpose, and only



It may be adopted when there are no alternative means that are less invasive or restrictive to achieve the same objective, in compliance with the principle of human rights protection.

IV. Human Rights: Artificial intelligence must guarantee full respect for the human rights recognized in the Political Constitution of the United Mexican States, the international treaties to which the Mexican State is a party, and other applicable regulations. Its use may not justify the violation of civil, political, social, economic, cultural, or digital rights.

V. Legality: Any use of artificial intelligence must be based on clear, accessible, and predictable legal standards, in accordance with the applicable constitutional and legal framework, and with respect for human rights.

VI. Explainability and Algorithmic Transparency: Artificial Intelligence systems must operate under mechanisms that allow their decisions, internal processes, and operating criteria to be understood, with the aim of ensuring accountability, effective supervision, and the right to information of users or affected parties.

VII. Responsibility and Accountability: Any natural or legal person, public or private, that develops, implements or uses Artificial Intelligence systems will be legally responsible for their effects, impacts and automated decisions, and must be held accountable for any damages or consequences that such systems may cause.

generate.

VIII. Non-Discrimination and Algorithmic Justice: Artificial Intelligence systems must be designed and implemented in such a way as to avoid any type of direct or indirect discrimination, whether based on ethnic origin, gender, sexual orientation, age, social status, disability, or any other personal condition or circumstance.



IX. Equity and Social Inclusion: Artificial intelligence should contribute to reducing social, economic, generational, technological, and cultural gaps, promoting access to and benefits for all people, especially those belonging to historically disadvantaged groups.

X. Meaningful Human Oversight: Any automated decision that has significant legal, social or personal consequences must have effective human oversight, capable of intervening, correcting or reversing its results when necessary to protect rights or the public interest.

XI. Environmental Sustainability: The development and use of artificial intelligence must be consistent with environmental protection, mitigation of the ecological footprint, and compliance with international commitments regarding climate and sustainable development.

XII. Best Interests of Children: Any application of artificial intelligence that may directly or indirectly affect children or adolescents must prioritize the principle of the best interests of children, guaranteeing their physical, mental, emotional, and digital protection.

XIII. Democratic and Plural Participation: The regulation, supervision and governance of artificial intelligence must include the effective participation of civil society, academia, indigenous peoples, the private sector and other social sectors, based on criteria of plurality, equity and informed deliberation.

XIV. Plurality: It requires ensuring the participation and inclusion of different social, academic, scientific, technical, and cultural sectors in the design, regulation, and implementation of artificial intelligence technologies, avoiding single or hegemonic visions.

XV. Caution and Proportionality in Innovation: In the face of emerging risks, technological innovation must be guided by the precautionary principle, avoiding implementing technologies without



prior ethical, social, and environmental impact assessments. Regulatory measures must be proportional to the level of risk identified.

XVI. International Cooperation and Technological Multilateralism: Mexico will actively participate in multilateral forums on artificial intelligence through the practice of International Development Cooperation, collaborating in the design of global standards, promoting the exchange of good practices, and defending an approach based on human rights, peace, and the self-determination of peoples.

XVII. Pro-persona: In the interpretation and application of provisions relating to the development, implementation, and use of artificial intelligence systems, the provision that provides the broadest and most effective protection for people's human rights shall prevail. In case of doubt or conflict between standards, the one that favors greater dignity, freedom, integrity, and well-being of people should be chosen, prioritizing human interests over technological interests.

XVIII. Proportionality: Establishes that any measure adopted in relation to the use of artificial intelligence that affects rights must be appropriate, necessary and balanced with respect to the legitimate purpose pursued, avoiding excessive or arbitrary restrictions.

XIX. Protection of Personal Data: All processing of personal data in the development, implementation, and operation of artificial intelligence systems must be carried out respecting the rights to privacy, informational self-determination, and confidentiality of individuals. It requires that data be collected lawfully, fairly, and transparently; used only for legitimate, specific, and explicit purposes; and protected with appropriate technical and organizational measures, guaranteeing its security, integrity, and availability, and preventing unauthorized access, alteration, loss, or disclosure.



XX. **Shared Responsibility:** Recognizes that the various actors involved in the life cycle of artificial intelligence systems—designers, developers, suppliers, users, and authorities—share duties and obligations in preventing harm and protecting rights.

XXI. **Territorial and redistributive equity.** The use of artificial intelligence systems should help close social, economic, and technological gaps between regions, populations, and vulnerable groups.

XXII. **Algorithmic Sustainability:** The planning, development, and implementation of Artificial Intelligence systems must consider their energy, material, and environmental impact, favoring low-consumption models and green technologies.

XXIII. **Technological Sovereignty:** The State will promote national self-sufficiency in the design, control, and strategic use of artificial intelligence technologies, fostering scientific development, national innovation, and technological independence from external geopolitical or commercial interests.

XXIV. **Transparency:** Imposes the duty to ensure that processes, criteria, data, and decisions related to artificial intelligence systems are accessible, understandable, and auditable, allowing for accountability and public oversight.

CHAPTER IV – COMPETENT AUTHORITIES AND COORDINATION INTERINSTITUTIONAL

Article 7. The competent authorities for the application, supervision, promotion and surveillance of this Law are:

- The Federal Executive Branch, through the Ministry of the Interior, the Ministry of Economy, the Ministry of Public Education, the Ministry of Health, and other agencies involved in the development, use, or supervision of artificial intelligence.



- II. The Secretary of Anti-Corruption and Good Governance, through Transparency of the People.
- III. The National Human Rights Commission (CNDH), regarding the monitoring of respect for fundamental rights in the face of automated technologies.
- IV. The Federal Consumer Protection Agency (PROFECO) on the protection of users from artificial intelligence systems in products and services.
- V. The Secretariat of Science, Humanities, Technology and Innovation (SECIHTI), regarding scientific policy, technological development and national innovation.
- VI. The governments of the federal entities and Mexico City, within the scope of their respective powers.
- VII. The National Algorithmic Audit Platform (PNAA), as an autonomous technical body attached to the National AI Council, will be the competent authority to evaluate, diagnose, and issue technical opinions on artificial intelligence data sets, models, and systems, in accordance with the provisions of this Law.

Article 7 bis. The competent authorities in matters of rights protection, cybersecurity, children, the environment, consumer protection, personal data protection, law enforcement, as well as sectoral authorities with sanctioning powers, must **establish inter-institutional collaboration mechanisms with the National Council on Artificial Intelligence** and the PNAA, in order to guarantee:

- a) The incorporation of technical evidence in sanctioning procedures;
- b) The request for specialized algorithmic audits;
- c) The implementation of precautionary measures based on technical findings;



d) The issuance of proportional sanctions based on technical opinions.

Article 8. The authorities mentioned in the previous article must coordinate to:

- I. Design and implement comprehensive public policies on artificial intelligence.
- II. Establish common criteria for risk classification, technical supervision, auditing, accountability and protection of rights.
- III. Share information, best practices, and monitoring results on the impact of Artificial Intelligence in their respective areas of activity.
- IV. Coordinate actions to prevent, investigate, and punish improper, abusive, or illegal uses of artificial intelligence systems.
- V. Promote regulatory harmonization and collaboration with international organizations, research centers and technological innovation networks.

Article 9. The Federal Executive may create, through regulatory provisions, specialized administrative units or national artificial intelligence innovation centers, the National Artificial Intelligence Council, for the purpose of:

- I. Provide technical support to agencies and entities in the implementation of this Law.
- II. Conduct algorithmic impact assessments and audits specialized.
- III. Propose technical standards, analysis methodologies and certification criteria.



IV. Coordinate with the National Council on Artificial Intelligence, in accordance with the following chapter.

CHAPTER V – NATIONAL COUNCIL OF ARTIFICIAL INTELLIGENCE

Article 10. The National Council for Artificial Intelligence is hereby created as a decentralized public body of the Federal Public Administration, non-sectorized, with legal personality and its own assets, technical and management autonomy, and domiciled in Mexico City.

Its purpose is to advise the competent authorities on the design, monitoring, and evaluation of public policies, regulations, and strategies related to artificial intelligence, in accordance with the principles established in this Law.

Article 11. The National Council for Artificial Intelligence shall have the following powers:

- I. Advise the Federal Executive and the competent agencies on public policies, regulations and national strategies for artificial intelligence.
- II. Coordinate the development of technical guidelines and criteria for the design, use, and supervision of artificial intelligence systems, promoting their transparency, security, and respect for human rights.
- III. Promote scientific, technological, and innovative development in the field of artificial intelligence, in collaboration with public, academic, and private institutions.
- IV. Promote international cooperation in artificial intelligence, in coordination with the Ministry of Foreign Affairs, to foster the exchange of good practices, ethical standards, and innovation projects.
- V. Issue an annual public report on the general status of artificial intelligence in Mexico, including progress, challenges, and strategic recommendations.



VI. Establish technical consultation or collaboration committees to strengthen the national artificial intelligence ecosystem, integrating the public, social, and private sectors.

VII. Promote open access to the results of publicly funded artificial intelligence research and development projects, in accordance with applicable legislation.

VIII. Carry out other activities that this Law and other provisions legal powers conferred upon it for the fulfillment of its purpose.

Article 12. The assets of the National Council shall be composed of the following: I. The movable and immovable property assigned to it by the Federal Government, and any property acquired by any legal title, and II. The transfers, subsidies, donations, and legacies it receives, as well as, in general, the income it obtains from consultations, expert reports, royalties, recoveries, intellectual property rights, or any other service or concept specific to its purpose. The National Council shall administer and dispose of its assets in the fulfillment of its purpose, in accordance with applicable legal provisions.

Article 13. The National Council shall have an oversight body composed of a Public Commissioner and an alternate, appointed by the Secretariat of Public Service, who shall have the powers granted to them by the Federal Law on Parastatal Entities and other applicable legal provisions.

The National Council will have an Internal Oversight Body that will report hierarchically, functionally, and budgetarily to the Secretariat of Public Service.

Public servants assigned to the Internal Control Body, within the scope of their powers, shall exercise the powers provided for in the Organic Law of the Federal Public Administration, the Federal Law on Parastatal Entities, and the General Law on Administrative Responsibilities, as well as in other applicable legal and administrative regulations.



Article 14. The Director General shall establish the general working conditions of the National Council, subject to authorization from the Ministry of Finance and Public Credit in accordance with applicable legal provisions. The working relationship between the National Council and its employees shall be governed by the provisions of Article 123, Section B, of the Political Constitution of the United Mexican States.

Article 15. The National Council for Artificial Intelligence will be composed of multi-sectoral and equal members:

- Representatives of federal executive agencies and entities with expertise in artificial intelligence, innovation, science, technology, human rights, education, the environment, security, and strategic sectors.
- II. Representatives of the Legislative and Judicial branches invited on an honorary basis.
- III. Experts in ethics, law, data science, human rights, the environment, education, architecture, urban planning, security, emerging technologies, and relevant industrial sectors.
- IV. Representatives of academic institutions, research centers, and public and private universities.
- V. Representatives of civil society organizations, indigenous peoples, technology communities, and citizen groups.
- VI. Representatives of the business sector, especially from technology industries, national innovation, territorial planning, and digital transformation.
- VII. A Technical Secretariat, appointed by a qualified majority of the Council itself, responsible for operational functions, monitoring of agreements and institutional liaison.



The Council must strive, at all times, to achieve gender parity, as well as diverse territorial, cultural, and sectoral representation from Mexico in its membership.

Article 16. The members of the National Council on Artificial Intelligence will be appointed for a five-year term, with the possibility of being renewed for a single additional immediate term.

The procedure for appointing, renewing, and removing members will be established in the Council's Organic Statute, in accordance with the principles of transparency, merit, gender parity, and sectoral diversity.

Participation in the Council will be honorary and will not generate remuneration, except for those operational functions of the Technical Secretariat, in accordance with budgetary availability.

Article 17. In order to fulfill its purpose, the National Council will have the following basic structure:

- VO. A General Directorate, headed by a titular person, responsible for the legal representation, strategic management and general administration of the organization.
- II. The Governing Body of the Council, formed in a multi-sectoral manner in accordance with the provisions of this Law.
- III. A Technical Secretariat, responsible for internal operations, session preparation, monitoring of agreements, and inter-institutional coordination.
- IV. A Supervisory Body, composed of a Public Commissioner and a substitute, appointed by the Secretariat of Public Service.
- V. An Internal Control Body, dependent on the Secretariat of Public Function, which will exercise the oversight functions,



internal control and prevention of administrative liabilities.

- VI. The administrative units necessary for the exercise of its substantive and support functions.

The Organic Statute of the National Council will specify the organization, operation, and specific powers of each body, guaranteeing maximum efficiency, impartiality, transparency, and respect for human rights.

Article 18. The functions of the Council are:

- VO. Issue non-binding technical opinions and recommendations on the development and implementation of this Law.
- II. Propose ethical, technical, and legal criteria for risk assessment, system certification, algorithmic audits, and damage repair mechanisms.
- III. Evaluate the social, economic, environmental and cultural impact of the implementation of artificial intelligence in Mexico.
- IV. Promote spaces for public deliberation, citizen participation, and free, prior, and informed consultation with affected communities.
- V. Recommend public policy measures that promote responsible innovation, technological sovereignty, and digital inclusion.
- VI. Issue annual reports on the state of artificial intelligence in Mexico, which are public.
- VII. Establish coordination mechanisms with multilateral organizations, cooperation agencies, and international algorithmic governance networks.



VIII. Design specific public policies to promote the development of Artificial Intelligence solutions by national micro, small, and medium-sized enterprises, with an emphasis on social impact and sustainable development.

IX. Recommend the adoption, modification, or development of regulatory frameworks and public policies related to the development, implementation, and supervision of artificial intelligence systems, in accordance with the principles established in this Law.

X. Promote the incorporation of artificial intelligence in territorial development and urban planning, driving the construction of people-centered smart cities, based on principles of sustainability, equity, accessibility and resilience.

Article 19. The Council shall meet at least twice a year and may call extraordinary sessions when so determined by its board.

directive.

Their opinions and recommendations will be adopted by majority vote and will be public.

The members will participate on an honorary basis, except for the Technical Secretariat.

The Council may invite national and international experts or institutions as observers or temporary advisors.

Article 20 The National Council for Artificial Intelligence will promote, in coordination with the competent authorities of the federal entities, the creation of State Review Councils for Artificial Intelligence, of an honorary and advisory nature.

These State Councils will have the following purposes:

- 10. Analyze problems, cases and good practices related to the development, implementation and supervision of artificial intelligence systems in their respective entities;



- II. Formulate proposals for local regulations, guidelines or points of agreement that contribute to the proper application of this Law at the state level;
- III. Coordinate with the National Council on Artificial Intelligence through communication mechanisms established in the respective Organic Statute.

Participation in the State Councils will be honorary and will not generate any remuneration.

CHAPTER VI – OF THE NATIONAL ALGORITHMIC AUDIT PLATFORM

Article 21. The National Algorithmic Audit Platform (PNAA) is hereby created as a specialized technical body, with technical and operational autonomy, attached to the National Council for Artificial Intelligence.

The PNAA aims to evaluate public and private training datasets, artificial intelligence architectures, and systems to ensure compliance with the principles of equity, transparency, explainability, traceability, non-discrimination, and protection of fundamental rights.

To fulfill its functions, the PNAA may develop, implement, use, or contract technological tools, including those based on artificial intelligence, automated data analysis, algorithmic auditing, and systemic risk detection, in accordance with the principles and provisions of this Law.

The PNAA must maintain its technological capabilities, methodologies, and tools up to date to preserve their effectiveness, reliability, and compliance with the state of the art in artificial intelligence and algorithmic auditing, in accordance with the principles of continuous improvement, responsible innovation, and the protection of fundamental rights.

The National Algorithmic Audit Platform (PNAA), in coordination with the National Council of Artificial Intelligence, must define, publish and periodically update the technical metrics, methodologies of



evaluation and international standards applicable to audits of artificial intelligence systems, ensuring objective, verifiable criteria in line with global best practices.

Article 22. The PNAA shall have the following functions:

- I. Audit datasets used to train AI models, identifying structural biases, deficiencies in representativeness, and risks of differentiated impact.
- II. Evaluate Artificial Intelligence models and systems using technical metrics of fairness, parity, explainability, and traceability.
- III. Issue public and technical reports, as well as assign algorithmic evaluation labels in accordance with the risk traffic light.
- IV. Validate the technical suitability of Artificial Intelligence systems before its registration in RENSIA.
- V. Provide self-assessment tools for developers public, private and academic.
- VI. Receive and address citizen complaints about unjustified, opaque, or discriminatory automated decisions.
- VII. Collaborate with national and international institutions in the generation of good practices, methodologies and open standards for algorithmic auditing.

Article 23. The PNAA will be coordinated by a Technical Directorate designated by the National Council of Artificial Intelligence.

It will have a Technical-Scientific Advisory Committee, made up of experts in data science, artificial intelligence ethics, digital law, sociology, territorial planning, economics, and public policy evaluation.



The operational, technical, and budgetary functioning of the PNAA will be regulated by the guidelines issued by the National AI Council.

Article 24. The reports, indicators, and risk labels generated by the PNAA shall be public and accessible, except in cases where there is a well-founded justification for reasons of national security, protection of personal data, or third-party rights.

The Platform will have a digital portal that allows for historical tracking of the audited systems, as well as public verification tools.

Article 25. Artificial intelligence systems classified as high risk must be assessed by the PNAA before being registered in the National Registry of Artificial Intelligence Systems (RENSIA), without prejudice to other internal or external audits that may be appropriate.

Article 26. The National Algorithmic Audit Platform may enter into collaboration agreements with autonomous bodies, academic institutions, civil society organizations, international organizations, and federal, state, or municipal regulatory authorities, with the aim of developing joint audits, strengthening their evaluation methodologies, implementing civic technologies, or promoting continuous improvement actions in the area of algorithmic auditing.

CHAPTER VII – SOCIAL PARTICIPATION AND TECHNICAL CONSULTATION

Article 27. Every person, organization, community, or collective has the right to participate in the consultation, design, evaluation, and oversight processes of public policies, standards, and programs related to artificial intelligence, in accordance with the principles established in this Law.

Article 28. The competent authorities shall ensure effective mechanisms for social participation, including:



- I. In-person or virtual public consultations for the development of standards, regulations, technical protocols and policies related to artificial intelligence.
- II. National, regional or sectoral deliberative forums organized by public agencies, academic institutions or the National AI Council.
- III. Technical working groups with representatives of indigenous peoples and comparable communities, guaranteeing prior, free, informed, and culturally appropriate consultation when dealing with technologies that may impact their collective rights.
- IV. Open digital platforms for receiving comments, citizen proposals, and independent evaluations of artificial intelligence systems.
- V. Citizen or academic observatories, specialized in AI monitoring, integrated through public and transparent calls.

Article 29. Opinions, proposals and observations received through the participation mechanisms must:

- I. Be incorporated in a reasoned manner in the final documents, specifying whether they were accepted or rejected and with what justification.
- II. Be available for public consultation in accessible formats, including versions in indigenous languages where appropriate.
- III. Be considered as part of the social and ethical impact assessment of regulated Artificial Intelligence systems.

Article 30. The authorities shall promote digital literacy and social understanding of artificial intelligence programs, in order to:



Strengthen informed citizen participation in regulatory processes.

Guarantee the right to knowledge and understanding of automated systems that impact everyday life.

Combat disinformation, technophobic or technocratic myths, and promote a critical, ethical, and democratic approach.

CHAPTER VIII – RISK TRAFFIC LIGHT SYSTEM

Article 31. All artificial intelligence systems operating in Mexico, whether developed in Mexico or implemented by foreign actors, must be classified according to the Risk Traffic Light System, which is composed of the following categories:

- I. Minimum risk AI
- II. Limited risk AI
- III. High-risk AI
- IV. Prohibited AI

Article 32. The classification will be determined according to the following criteria:

- I. The system's ability to generate automated decisions with legal or material consequences for individuals or legal entities.
- II. The degree of functional autonomy that the system presents.
- III. The potential impact on fundamental rights, health, life, liberty, privacy, dignity, equity or the environment.
- IV. The use of the system in sensitive contexts: justice, public safety, health, education, democratic processes, financial services or vulnerable populations.



- V. The possibility of psychological manipulation, mass surveillance, algorithmic discrimination or data exploitation without informed consent.

Article 33. Categorization by risk level

I. **Low-risk AI:** Systems without significant potential for harm to rights or people. They do not require special authorization or oversight, but must observe general principles of the Law.

II. **Limited-risk AI:** Systems that can generate moderate effects. They require basic transparency mechanisms such as user warnings, minimal explanations, and mitigation measures.

III. **High-risk AI:** Systems capable of producing serious or irreversible consequences. They are subject to:

- a. Prior assessment of algorithmic impact
- b. Periodic technical and legal audits
- c. Mandatory registration with the competent authority
- d. Continuous supervision
- e. Obligations of robust traceability and explainability

IV. **Prohibited AI:** Systems whose operation is expressly prohibited by this Law due to their unacceptable risk. Their development, commercialization, use, or implementation are subject to administrative, civil, and criminal sanctions.

Article 34. The classification of an artificial intelligence system may be reviewed by the competent authorities based on:

- I. New data on its operation, effects or social impact.
- II. Scientific or technological advances that modify your level of risk.
- III. Citizen reports, academic research or complaints.
- IV. International regulatory changes adopted by Mexico.



The National Council for Artificial Intelligence must review and, where appropriate, update the categories and criteria of the Risk Traffic Light System at least every two years, in accordance with scientific and technological advances, international recommendations, and empirical evidence. These updates must be subject to public consultation and a technical opinion from the National Algorithmic Audit Platform.

CHAPTER IX – OBLIGATIONS BY RISK LEVEL

Article 35. Regardless of their level of risk, all artificial intelligence systems shall be subject to the following minimum obligations:

- I. Respect the guiding principles established in this Law.
 - II. Guarantee the right to privacy, personal data protection, and digital security.
 - III. Avoid the generation of unjustified biases, discrimination or exclusion.
 - IV. Inform in a clear and accessible manner when a person is interacting with an automated system.
 - V. Do not induce harmful, self-destructive, violent or manipulative.
 - VI. Ensure that the information and results generated by the system are verifiable and transparent in their methodology.
- Provide training and resources to users to facilitate safe and appropriate use.

Article 36. In addition to the general obligations, systems classified as limited risk must:

- I. Include functional transparency mechanisms that allow the user to understand that they are interacting with an AI.
- II. Provide access to basic information on the operation, purpose and limitations of the system.



III. Allow the option to disconnect or not participate, when appropriate technically possible.

IV. Take reasonable measures to prevent misuse or misrepresentation of the results.

Article 37. Systems classified as high risk shall be subject to the following reinforced obligations:

I. Have an algorithmic impact assessment prior to implementation.

II. Be registered with the competent authority in accordance with the procedure established by the regulations of this Law.

III. Be subject to periodic technical audits, including those carried out by the National Algorithmic Audit Platform, in accordance with the guidelines issued for this purpose.

IV. Ensure meaningful human oversight of any automated decision that may affect fundamental rights.

V. Implement technical and legal traceability and explainability mechanisms, adapted to different user profiles.

VI. Establish update, security, and reporting protocols incidents and care for affected people.

VII. Certify that the training data is representative, ethical, verifiable and free of structural biases.

VIII. Ensure the right of people to access, question and appeal automated decisions that affect them.



Article 38. The development, training, implementation, use, marketing, import or export of artificial intelligence systems that:

- I. Use subliminal manipulation techniques or extreme psychological persuasion to alter human behavior without consent.
- II. Establish mechanisms for coercive social scoring by from public or private entities.
- III. Carry out mass biometric surveillance in public spaces without express judicial authorization and strict institutional control.
- IV. Exploit the vulnerabilities of people with disabilities, minors, the elderly, or those in situations of psychosocial vulnerability.
- V. Generate simulated audiovisual or textual content for the purposes of fraud, disinformation or digital violence, without authentication or visible labeling mechanisms.

Failure to comply with this provision will result in administrative, civil, and criminal sanctions, in accordance with the provisions of this Law, international treaties, and other applicable regulations.

CHAPTER X – NATIONAL REGISTER OF INTELLIGENCE SYSTEMS ARTIFICIAL

Article 39. The National Registry of Artificial Intelligence Systems (RENSIA) is hereby created as a public, technical, and up-to-date database, managed by the competent authority, which will contain key information on artificial intelligence systems classified as high risk or developed by public entities.

It is an essential requirement to have been evaluated by the National Algorithmic Audit Platform, which will issue a risk assessment that will be part of the registration file.



Article 40. *The Registry shall have the following purposes:*

- I. Promote transparency in the use of Artificial Intelligence systems in sensitive sectors.
- II. Facilitate public auditing, institutional oversight and academic research.
- III. Guarantee the right of people to know about Artificial Intelligence systems that impact their lives, their environment, or their rights.
- IV. Serve as a tool for inter-institutional coordination and management of algorithmic risk.
- V. Encourage good practices in ethical and responsible technological development.

Article 41. The Registry must contain, at least, the following information:

- I. Name, type and purpose of the artificial intelligence system.
- II. Risk level classified according to the legal traffic light.
- III. Name of the developer, supplier or responsible entity.
- IV. Sector or scope of application.
- V. Specification as to whether or not there is significant human intervention.
- VI. Impact and results evaluation methodology.
- VII. Basic technical data, including the type of algorithms used.
- VIII. Date of registration, updates and operational status of the system.



IX. Appeal or contact mechanisms for users or individuals affected.

X. Measures taken in case of incidents, failures, biases or damages.

Article 42. Public access and data protection

ya. The Registry will be publicly accessible, free of charge, and searchable online, except for information that, pursuant to law, is classified for reasons of national security, technical confidentiality, or personal data protection.

II. Public versions of the Registry must guarantee accessibility, citizen language, open formats, and thematic search engines.

III. Individuals or legal entities may request clarifications, rectifications, or justified cancellations in the exercise of their right to data protection and access to information.

Article 43. Obligated entities must keep the information registered in the Registry updated, at least annually or after each significant modification to the system.

The authority responsible for RENSIA will conduct random checks and technical audits, and may impose corrective measures or sanctions in the event of omissions, falsifications, or negligence.

CHAPTER XI – RIGHTS OF USERS AND AFFECTED PERSONS

Article 44. Any person who interacts, directly or indirectly, with an artificial intelligence system shall have the following rights, without prejudice to those already established in other laws:

I. People have the right to be informed, in a clear, accessible, and understandable manner, when they are interacting with an artificial intelligence system, as well as about its purpose, general operation, limitations, and the person responsible for it.

When the interaction involves automated decisions with



significant effects, the information must include the legal basis, the general criteria of the algorithm and the means of challenge or review.

- II. No artificial intelligence system may discriminate on the basis of ethnic origin, gender, age, religion, sexual orientation, disability, socioeconomic status, ideology, language or any other protected category. People affected by

Discriminatory automated decisions may require the suspension of the system, correction of the results and, where appropriate, compensation for the damage.

- III. Individuals have the right to have significant decisions affecting them not made exclusively by automated systems, but rather to have meaningful human oversight. Upon request, individuals should be able to receive assistance, advice, or review from a trained human operator in the relevant system.

- IV. Everyone has the right to know, in a reasonably understandable language, the reasons or criteria behind automated decisions that significantly affect them. Competent authorities must ensure that high-risk systems have technical and legal explainability mechanisms tailored to specific profiles: ordinary citizens, technical users, judges, auditors, or authorities.

- V. Individuals shall have the right to appeal, question, or challenge any relevant decision made, in whole or in part, by an artificial intelligence system. The review procedure shall ensure reasonable timeframes, free access, non-retaliation, and the possibility of reversing or modifying the decision.

- VI. Data processed by Artificial Intelligence systems must comply with Mexican legislation on personal data protection. Individuals have the right to access, rectify, erase, object to, and transfer their data, including in automated processes.



VII. Any person who suffers physical, moral, patrimonial, or symbolic harm as a result of the use of an artificial intelligence system shall have the right to full, effective, and proportional reparation for the harm caused. Reparation may include: restitution, compensation, rehabilitation, satisfaction, and guarantees of non-repetition.

CHAPTER XII – OBLIGATIONS OF DEVELOPERS, OPERATORS AND INSTITUTIONAL USERS

Article 45 The following are subject to the provisions of this chapter:

- I. Individuals or legal entities, national or foreign, that develop, design, train, adjust, use or market artificial intelligence systems that operate in Mexico.
- II. Public or private entities that implement, integrate, or use artificial intelligence systems in decision-making, interaction, or analysis processes involving Mexican individuals or legal entities.
- III. Human operators, technicians or administrative personnel who actively participate in the supervision, control or application of such systems.

Article 46. Those who develop artificial intelligence systems must:

- I. Incorporate principles of ethics, human rights, non-discrimination and digital security.
- II. Carry out technical and legal impact assessments before the commercialization or implementation of the system.
- III. Avoid using training data that reproduce biases unjustified or structural errors.



- IV. Provide clear and up-to-date technical documentation on the operation of the system.
- V. Design mechanisms that allow explainability, traceability and reversibility of the results.
- VI. Implement continuous improvement, monitoring, and updating processes, especially in dynamic systems or those that learn in real time.
- VII. Ensure that, in cases defined as high risk, data sets and digital architectures are evaluated in accordance with the technical guidelines issued by the National AI Council.
- VIII. In the cases provided for by this Law, the Platform may intervene National Algorithmic Audit.

Article 47. Entities or persons that use Artificial Intelligence systems to offer public or private services must:

- I. Ensure that the systems used have been registered, evaluated and classified in accordance with this Law.
- II. Clearly inform users about the existence, functions and limits of the automated system.
- III. Establish meaningful human oversight mechanisms, especially when rights are violated.
- IV. Have accessible channels for attention, appeals and reparation and effective.
- V. Report any incident, failure, detected bias or negative impact to the corresponding authority.



VI. Train your technical, legal and operational staff in the ethical use and legal of artificial intelligence.

Article 48. When the Mexican State or its dependencies use AI systems, they will be obliged to:

- I. Ensure strict compliance with this Law and all constitutional principles.
- II. Prioritize the use of systems developed or validated by national institutions whenever possible.
- III. Conduct public audits and periodic accountability on the performance of AI systems.
- IV. Ensure that there are no negative impacts on vulnerable groups, indigenous populations, or people in disadvantaged situations.
- V. Avoid any form of mass surveillance, institutional bias, algorithmic manipulation or injustice.
- VI. Promote open access to data, methodologies, and algorithms, except for legally justified reasons.

Article 49. Any artificial intelligence system classified as high risk or used in sensitive sectors must have an Algorithmic Impact Assessment (EIA) prior to its implementation.

The EIA shall consider at least:

- I. Purpose of the system and context of use.
- II. Types of data used, sources and processing.
- III. Affected populations and differentiated risks (gender, age, disability, ethnicity).



IV. Possible impacts on human rights, health, assets, dignity, privacy or reputation.

V. Mitigation measures, human supervision and protocols revision.

The evaluation must be prepared by a multidisciplinary team and submitted to the competent authority for review and registration.

In dynamic systems or those capable of continuous learning, the EIA must be updated periodically.

Article 50. Persons or entities responsible for Artificial Intelligence systems must have an incident response protocol, which includes:

- I. Identification, containment and immediate correction.
- II. Mandatory notification to users or affected persons.
- III. Technical report to the competent authority within 72 hours hours following the incident.
- IV. Measures to prevent the event from recurring.

Incidents must be documented and retained for a minimum of five years.

In the event of serious risks or imminent damage, the authority may suspend the operation of the system as a precautionary measure.

Article 51. In sectors such as health, justice, education, public security, financial services or labor, reinforced obligations will apply, including:



I. Prohibition of automated decisions without human intervention when they involve significant impacts on rights.

II. Mandatory registration with the competent authority and RENSIA.

III. Direct supervision by internal control bodies and committees ethics.

IV. Prior consultation with users or communities impacted, where appropriate.

Under no circumstances may Artificial Intelligence be used to automate criminal trials, issue diagnoses without medical review, grade students without teacher supervision, or deny essential public services without human evaluation.

Responsible entities must submit their systems to periodic evaluation by the PNAA when applying them in priority sectors defined by the National Council.

CHAPTER XIII – RESPONSIBILITY AND ACCOUNTABILITY ALGORITHMIC

Article 52. Any natural or legal person, public or private, that develops, implements, controls or operates an artificial intelligence system shall be liable for any damages caused by said system to persons, property, rights or legally protected interests.

Liability will be objective in nature, without the need to demonstrate intent or negligence, when it comes to high-risk systems.

The foregoing is understood without prejudice to any corresponding criminal, administrative or civil liability.

Article 53. When multiple persons or entities participate in the development, implementation or use of an Artificial Intelligence system, they will be jointly and severally liable to the affected persons, unless otherwise provided.



demonstrate with conclusive evidence a clear division of functions and effective controls.

Article 54. To determine the existence and scope of liability, the following must be considered:

- VO. The risk level of the system and whether it had the corresponding classification, certification or evaluation.
- II. Compliance or non-compliance with the obligations established in this Law.
- III. The existence of human supervision, traceability and explainability mechanisms.
- IV. The foreseeability of the damage and the reasonable preventive measures adopted.
- V. The economic or functional benefit obtained from the use of the system.

Article 55. Public and private entities that operate Artificial Intelligence systems must guarantee internal and external accountability mechanisms, including:

- I. System operating records.
- II. Auditable access to automated decisions.
- III. Designation of internal responsible persons.
- IV. Accessible reporting and complaint channels.

Failure to register, document, or cooperate with audits will be considered a presumption of non-compliance.

Article 56. Establishes the right of affected persons to demand reparation and use courts, public defenders' offices, autonomous bodies and administrative mechanisms.



Article 57. Persons affected by the development, implementation, or use of artificial intelligence systems shall have the right to access courts, public defenders' offices, autonomous bodies, and administrative complaint mechanisms to demand full reparation for damages.

They may request compensation for damages to their human, property, emotional rights, access to services, or any other harm resulting directly or indirectly from automated decisions or actions.

Article 58. The competent authorities shall:

- VO. Ensure accessible, expeditious, and effective resources tailored to the technical characteristics of the artificial intelligence systems involved.
- II. Adopt collective measures when damage systematically affects vulnerable groups of people, communities, or social sectors.
- III. Apply the pro-persona principle and presume the existence of harm when there is algorithmic opacity, technical asymmetry, or a reasonable impossibility of directly verifying the damage.
- IV. Accept the findings of technical audits conducted by the National Algorithmic Audit Platform (PNAA) as expert evidence in administrative or judicial proceedings.

Comprehensive reparation may include, depending on the case:

- I. Economic compensation proportional to the damage suffered;
- II. Full restitution of violated rights;
- III. Correction, limitation or deactivation of the system causing the damage;



IV. Imposition of administrative or public sanctions on those responsible;

V. Issuance of non-repetition guarantees.

Article 59. In judicial or administrative proceedings related to possible damages generated by artificial intelligence systems, the competent court or authority may:

- I. Order the technical and controlled opening of the model or system, even if it is private property.
- II. Request specialized expert reports to analyze the system's behavior, its training, its biases, and the traceability of its decisions.
- III. Demand the delivery of records, logs or technical evidence that allows determining the origin of the damage.

This power will be exercised with strict confidentiality, protection of intellectual property and third-party rights, in accordance with the principles of proportionality, necessity, and legality.

Article 60. Artificial intelligence systems classified as high risk must generate and maintain a continuous technical record (algorithmic record) of their operations, decisions, inputs and outputs, in a chronological, auditable and secure manner.

This record must:

- I. Identify the system and version used,
- II. Record relevant events and automated decisions,
- III. Be available for internal, external or judicial audits,



IV. To be kept for at least five years.

Failure to comply with this obligation will be considered obstruction of accountability.

Compliance with these principles may be technically and methodologically verified by the National Algorithmic Audit Platform.

Article 61. The creation of an Algorithmic Reparation Fund, of a public or mixed nature, is hereby authorized, intended to guarantee access to reparation for persons affected by Artificial Intelligence systems when:

- I. The person responsible cannot be identified with certainty,
- II. There are technical or legal barriers that prevent access to the justice,
- III. The responsible party has disappeared, gone bankrupt or is insolvent.

The fund may be fed by:

- a) State budgetary contributions,
- b) Fines imposed for non-compliance with this Law,
- c) Contributions from technology platforms or developers registered,
- d) Donations, agreements and international funds.

Its operation, access mechanisms and accountability will be regulated by specific regulatory provisions.



CHAPTER XIV – PROTECTION OF GIRLS, BOYS AND ADOLESCENTS

Article 62. In any action related to the development, implementation or use of artificial intelligence systems that may directly or indirectly affect girls, boys or adolescents, the principle of the best interests of the child must prevail as the primary criterion for the interpretation, application and implementation of this Law, in accordance with Article 4 of the Constitution and the General Law on the Rights of Girls, Boys and Adolescents.

Likewise, the use of artificial intelligence systems that contribute to the comprehensive development of children in their cognitive, emotional, social, cultural, ecological, and spiritual dimensions will be prioritized.

Article 63. The use of artificial intelligence systems that:

- VO. Generate, recommend or disseminate content that promotes violence, self-harm, hatred, discrimination or harmful behavior;
- II. Stimulate digital addictions, technological dependence or serious emotional disturbances;
- III. Promote psychological manipulation, disproportionate commercial exploitation, or dissemination of false, distorted, or decontextualized information that negatively affects the comprehensive development of minors;
- IV. Monitor, manipulate or profile girls, boys or adolescents for commercial, political or social control purposes;
- V. Generate or disseminate child sexual exploitation material, including content generated using hyperrealism techniques such as so-called deep lies
- VI. Exploit cognitive or emotional vulnerabilities inherent in childhood;



- VII. Train artificial intelligence models using data from minors without the express, informed, and verifiable consent of the person exercising parental authority, custody, or guardianship.

Artificial intelligence systems accessible to minors must incorporate age verification mechanisms, parental filters, default safe settings, explainability adapted to children, and pedagogical validation in accordance with principles of epistemic equity, cultural diversity, and neuroeducation.

Article 64. Natural or legal persons, national or foreign, that design, implement or provide artificial intelligence services accessible to minors must:

- I. Conduct a specific assessment of the impact on children's rights;
- II. Consult with specialists in childhood, pedagogy and human rights;
- III. Publish simplified and adapted versions of terms and conditions of use;
- IV. Prioritize secure configurations by design and implement opt-out mechanisms;
- V. Apply principles of privacy, security, and enhanced accessibility, even when operating from abroad, in accordance with the principles of digital extraterritoriality and shared responsibility.

In school settings, they must also:

- I. Integrate artificial intelligence systems into pedagogical plans approved by the competent national authorities;



- II. Have interdisciplinary teams for emotional, ethical and social monitoring;
- III. Provide ongoing training processes in artificial intelligence for teaching staff, families, and school communities.

Article 65. The Mexican State will promote the development, validation and implementation of artificial intelligence technologies in the educational field that:

- yo. Strengthen national technological sovereignty applied to pedagogical processes;
- II. Guarantee universal access to training platforms developed in Mexico;
- III. Link artificial intelligence with meaningful learning and cultural regeneration.

Any educational artificial intelligence should foster critical thinking, creativity, and emotional intelligence, integrating the significant presence of trainers, tutors, or guides who facilitate emotional support, critical reflection, and personalized follow-up.

Likewise, mechanisms for scheduled digital disconnection and offline activities that balance technological use with the comprehensive development of children and adolescents should be incorporated.

Article 66. Every artificial intelligence system accessible to or directed at minors must have a Child Algorithmic Impact Assessment that includes:

- yo. The analysis of emotional, cognitive, social and cultural risks derived from their interaction;
- II. The identification of interactions that involve the exercise of authority, behavioral encouragement or persuasion over minors;



- III. The detection of possible biases, stigmatization or prolonged exposure;
- IV. The definition of mitigation and adaptation measures in accordance with the evolutionary development of girls, boys and adolescents.

The Childhood Algorithmic Impact Assessment must be public, updated periodically, and validated by accredited child development professionals.

Article 67. The National Algorithmic Child Alert Mechanism is hereby created, coordinated by the Federal Attorney's Office for the Protection of Girls, Boys and Adolescents in collaboration with the National Council for Artificial Intelligence, whose functions will be:

- VO. Receive reports about algorithms, content or platforms that pose a risk to minors;
- II. Issue alerts and order the immediate suspension of reported systems when there is a serious risk;
- III. Publish binding recommendations for platforms and developers;
- IV. Ensure the protection of whistleblowers and the confidentiality of affected minors.

Likewise, the authorities will promote the right of children and adolescents to participate in the evaluation and improvement of artificial intelligence systems that affect them, through:

- VO. Forums adapted to your age and context;
- II. Consultations on perception and digital well-being;
- III. Critical, ethical and creative literacy programs on artificial intelligence;



IV. Representation spaces in advisory bodies linked to this Law.

Participation will be voluntary, protected, and accompanied by informed adults.

Article 68. Every Artificial Intelligence system accessible or directed at children or adolescents must have a Child Algorithmic Impact Assessment, which includes:

- I. Emotional, cognitive, social and cultural risks.
- II. Interactions that involve authority, behavioral encouragement or persuasion.
- III. Possible biases, stigmatization or prolonged exposure.
- IV. Mitigation measures and design adapted to evolutionary development.

This assessment must be published, periodically updated, and validated by accredited childhood professionals.

Article 69. The National Algorithmic Alert Mechanism for Children is hereby created, coordinated by the Federal Attorney's Office for the Protection of Children and Adolescents, in collaboration with the National Council for Artificial Intelligence, with the following functions:

- I. Receive complaints about algorithms, content or platforms harmful to minors.
- II. Issue alerts and order the immediate suspension of reported systems in the event of serious risk.
- III. Publish binding recommendations addressed to platforms and developers.
- IV. Ensure the protection of whistleblowers and the confidentiality of minors.



This mechanism will be accessible online, free of charge, and focused on prevention.

Article 70. Authorities shall promote the right of children and adolescents to participate in the evaluation and improvement of artificial intelligence systems that affect them, through:

- I. Forums adapted to your age and context.
- II. Consultations on perception and digital well-being.
- III. Critical, ethical and creative literacy programs on AI.
- IV. Representation spaces in advisory bodies linked to this Law.
- V. Training activities that include raising awareness about digital rights and the importance of their participation.
- VI. Access to secure digital platforms where they can share their experiences and concerns about the use of artificial intelligence.
- VII. Incentives for participation, such as public recognition or certifications that value their involvement in these processes.

All participation will be voluntary, protected and accompanied by informed adults.

Article 71. The National Council on Artificial Intelligence will annually prepare a National Report on the Impact of Artificial Intelligence on Children and Adolescents, which will include:

- I. Assessments of relevant policies, platforms and systems.
- II. Data on complaints, audits and recommendations issued.



III. Regulatory and public policy proposals for Congress and authorities.

IV. Participation of experts in childhood, mental health, education and technology.

The report will be public, in accessible formats, and will be submitted to Congress in the second half of each legislative year.

Article 72. The Mexican State will promote artificial intelligence at the service of educational sovereignty, prioritizing national technological developments that strengthen learning processes, educational equity, and the cultural regeneration of Mexican children and youth. All artificial intelligence applied to education must be designed from a perspective of human rights, inclusion, cultural diversity, neurodiversity, and emotional well-being.

Article 73. Artificial intelligence systems intended for use in school or community settings must:

- I. Promote critical thinking, creativity, intelligence emotional and peaceful conflict resolution.
- II. Respect the different learning rhythms and cognitive styles.
- III. Promote cultural identity, historical memory, and care for the environment and community collaboration.

Article 74. Every Artificial Intelligence system applied in formal or informal education must undergo a Child Educational and Emotional Impact Assessment (EIEEI), which includes:

- I. Analysis of the cognitive, emotional and social impact of the tool.



II. Pedagogical review by specialists in childhood and neuroeducation and critical pedagogies.

III. Cultural validation with indigenous peoples, community groups and school stakeholders.

Article 75. The use of automated systems in teaching-learning processes should never replace significant human presence.

The following must be guaranteed:

I. The figure of a tutor or guide with pedagogical and ethical training.

II. Feedback and emotional containment processes.

III. Time for digital disconnection and physical, creative and social activities. community.

Article 76. Expanded Data Protection and Children's Rights

Any use of Artificial Intelligence in educational platforms or systems that collect data from minors must:

Apply the principle of minimum data collection and maximum data protection.

Ensure informed and verifiable consent of guardians.

Ensure the right of children and adolescents to be digitally forgotten if they so require.

Article 77. The State shall promote, from early childhood, educational processes that:

Teach what Artificial Intelligence is in a critical, playful, and culturally situated way.

Develop deep digital ethics and conscious citizenship skills.



Empower children as co-creators, not just consumers, of technology.

Article 78. Artificial Intelligence for Regenerative Educational Communities

Artificial Intelligence developments that support:

Rural, indigenous, and popular schools with equitable access to smart resources.

Teaching processes contextualized in the natural and cultural environment.

Regenerative, cooperative, and intergenerational education networks supported by AI.

Article 79. The National Council for Artificial Intelligence may create a Certification Seal for Artificial Intelligence systems that:

Promote the comprehensive well-being of girls, boys and adolescents.

Be accessible, explainable and culturally relevant.

**CHAPTER XV – ARTIFICIAL INTELLIGENCE SYSTEMS IN SECTORS
STRATEGIC**

Article 80. The following sectors will be considered strategic for the regulation of artificial intelligence:

- I. Fundamental rights recognized in the Constitution are affected or in international treaties.
- II. Automated decisions are made with direct legal, health, educational, judicial, territorial planning, or economic consequences.
- III. There is a structural power relationship between the person who operates the system and the person affected.



IV. Sensitive, biometric, medical, and academic information is involved.
or judicial.

These include, but are not limited to: health, justice, education, public safety, labor, social protection, finance, the environment, and care for vulnerable groups.

Article 81. The use of artificial intelligence systems in strategic sectors—those where fundamental rights are affected or decisions of high social, legal, economic or vital impact are made—

must observe not only the general principles established in this Law, but also a reinforced set of ethical, technical and governance criteria, among which the following stand out:

I. Caution and gradual implementation: No system can be widely adopted without first going through stages of controlled testing, expert participation, and independent impact assessment.

II. Enhanced transparency: Systems must offer a level of explainability above the standard, allowing for a clear understanding of how they operate, the data used, and the assumptions underlying each result, ensuring that affected individuals have comprehensible access to this information.

III. Non-delegable human supervision: Ultimate responsibility for any high-stakes decision cannot rest exclusively on automated systems. A human with technical and legal training must validate, correct, or reverse the system's results when necessary.

IV. Informed and verifiable consent: In the processing of sensitive personal data—such as health, biometrics, cultural or ethnic identity—free, specific, informed consent must be obtained and recorded in a verifiable manner.

V. Prohibition of automation in irreversible decisions: Artificial intelligence systems are prohibited from making final decisions without



human intervention in matters such as complex medical diagnoses, court rulings, disciplinary measures or determinations that permanently affect the lives of people.

people.

Article 82. Any public or private institution that develops or implements artificial intelligence systems in strategic sectors must additionally comply with the following obligations:

10. Conduct a Specific Algorithmic Impact Assessment prior to adoption, which analyzes specific risks in relation to the environment, the affected population, the data used, and the foreseeable consequences.
- II. Register the system in the National Registry of Artificial Intelligence Systems (RENSIA), ensuring its traceability, public transparency, and regulatory oversight.
- III. Formally designate a person or team with technical, legal, and ethical training, responsible for the operational supervision of the system and the handling of incidents, failures, or disputes.
- IV. Submit periodic reports to the competent authority and the National Council on Artificial Intelligence, detailing the results obtained, errors detected, corrective measures implemented, and improvements made.
- V. Ensure that all users or affected persons have effective access to review, appeal, and redress mechanisms designed in an accessible, timely, and non-retaliation-free manner.

CHAPTER XVI – EXPLAINABILITY, TRANSPARENCY AND TRACEABILITY ALGORITHMIC

Article 83. Artificial intelligence systems must operate under a framework of enhanced transparency, which allows for understanding their



operation, audit its decisions, and, where necessary, assign responsibility. This involves ensuring:

- I. Functional transparency, meaning that every person clearly knows when they are interacting with an automated system and what degree of autonomy they have.
- II. Proportional explainability, adapted to the interlocutor's profile. What a person affected by an automated decision must understand is not the same as what a technical expert or a judge requires.
- III. Technical traceability, which allows for the reconstruction of system operations, its input data, decision criteria, and generated outputs. Traceability is an essential condition for detecting errors or biases and for implementing control mechanisms.
- IV. Differentiated accessibility, ensuring that transparency mechanisms are not reserved for experts, but are understandable and usable by the general public, authorities, and affected parties alike.

Article 84. Everyone has the right to know why and how an automated decision affecting them was made. This right is not incidental, but central in an environment where increasingly important processes are delegated to machines.

Therefore, the law recognizes that:

- I. People must be informed, in a clear and understandable way, when a relevant decision has been made in whole or in part by an AI system.
- II. They have the right to request and receive a reasoned explanation of the data used, the criteria applied, and the logic of the system that led to the decision.
- III. In the most sensitive cases, you have the right to have this explanation provided by a human being with the necessary training to clarify doubts, answer questions, and offer alternatives.



IV. Furthermore, they must have access to effective means of challenge, review, or appeal, especially if they believe the decision was erroneous, unfair, biased, or prejudicial.

Article 85. The obligation to provide explanations about the operation and decisions of artificial intelligence systems cannot be addressed uniformly. The needs, capabilities, and rights of those who interact with these systems vary considerably. Therefore, developers and operators will be required to ensure differentiated levels of explainability, tailored to the type of user, the context of use, and the level of impact that the automated decision may generate.

- I. **For the general public**, explanations must be written in clear and accessible language, avoiding unnecessary technical jargon. Practical examples, visual analogies, or graphic materials may be used to facilitate understanding of the basic functioning of the system, its purpose, and its limits.
- II. **For individuals directly affected by an automated decision**, a detailed and specific description of the process followed by the system must be provided: what data was used, how it was weighted, what criteria influenced the output generated, and what options exist to challenge, review, or reverse the decision.
- III. **For regulatory, judicial, or rights protection authorities**, systems must have sufficient technical documentation to allow for a complete analysis of their internal logic, model architecture, data source, and traceability of their results. This level of explainability must satisfy legal requirements and facilitate the attribution of liability in the event of a dispute.
- IV. **For technical experts and independent auditors**, tools must be made available to enable detailed algorithmic reviews. This includes access to performance metrics, information on potential biases detected, system validation and update processes, as well as any relevant documentation supporting its ethical, legal, and technical functioning.



In all cases, explainability is not only a right, but a fundamental component of public trust, accountability, and the prevention of harm resulting from the misuse of automated systems.

Article 86. Every limited or high risk artificial intelligence system must have the following minimum technical documentation:

- I. Purpose and functional scope of the system.
- II. Type of algorithms used and model versions.
- III. Sources, nature and quality of training data.
- IV. Performance, accuracy, bias and error evaluations.
- V. Results of internal or external audits.
- VI. Measures taken to ensure its explainability.
- VII. Relevant changes in its operation, configuration or architecture.

This documentation must be kept up-to-date, stored with security measures, and available for institutional review.

Article 87. High-risk Artificial Intelligence systems must generate an automated record that allows the reconstruction of decisions made, including:

- a) Relevant input data.
- b) Parameters and variables used.
- c) Output or result generated.
- d) Human intervention, if any.
- e) System identifier and its operating version.



f) Date, time and operating entity.

This record will have evidentiary value and must be kept for at least five years, or for the period established by sector regulations.

Article 88. The use of artificial intelligence systems that operate as black boxes, that is, without the technical, legal or practical possibility of:

- a) Explain its operation or decisions.
- b) Audit your models or data.
- c) Identify the source of errors or biases.

This prohibition will be especially enforceable when the systems are applied in strategic sectors or affect fundamental rights.

Article 89. Traceability will be a central element for:

- a) Determine liability in case of failure or damage.
- b) Correct systemic errors or unfair decisions.
- c) Evaluate the behavior of the system over time.
- d) Validate regulatory and ethical compliance.

Failure to comply with these provisions will be considered a presumption of opacity, negligence or bad faith, unless proven otherwise.

Article 90. The National Algorithmic Audit Platform (PNAA) may assess compliance with the provisions set forth in this chapter and incorporate its findings into the public risk reports it issues, in accordance with the principles of transparency, traceability, and accountability established in this legislation.



CHAPTER XVII – TECHNOLOGICAL SOVEREIGNTY AND NATIONAL DEVELOPMENT

Article 91. The State shall promote the development, implementation and use of artificial intelligence from a technological sovereignty perspective, understood as the national capacity to:

- I. Design and control your own AI systems.
- II. Develop our own algorithms, infrastructure and human talent.
- III. Guarantee critical independence from foreign platforms, models or suppliers.
- IV. Promote fair and equitable access to the benefits of technological development.

Article 92. The Federal Executive Branch shall develop, update, and implement, with the participation of the National AI Council, a National Strategy for Ethical and Inclusive Artificial Intelligence, which shall include:

- I. Diagnosis of the national AI ecosystem.
- II. Objectives, goals and priorities of technological development.
- III. Incentives for the development of talent, research and production national.
- IV. Lines of action for the public, ethical, and inclusive use of AI.
- V. Indicators of economic, social, environmental and social impact equity.

Article 93. The competent authorities shall promote the creation, consolidation and expansion of:



- I. New technology companies with an ethical and social focus.
- II. Open source and free software projects.
- III. Platforms national data, processing and storage.
- IV. National entrepreneurship and innovation networks.
- V. Cooperative or social enterprises in emerging sectors.

Article 94. In public contracts, acquisitions and projects involving artificial intelligence, preference shall be given to:

- I. Solutions developed by Mexican institutions.
- II. Auditable, adaptable models aligned with ethical principles.
- III. Projects that include participation of public universities, research centers or local groups.
- IV. Exceptions must be duly justified based on criteria of public interest or unavailable technical capacity.

CHAPTER XVIII – REGULATORY TESTING ENVIRONMENT AND INNOVATION CONTROLLED

Article 95. Artificial intelligence testing environments are controlled spaces for experimentation, created to allow the development and validation of emerging technologies under realistic but limited conditions. Through these environments, the State will facilitate responsible experimentation with innovative artificial intelligence systems, under flexible but supervised regulatory frameworks that prioritize safety, ethics, human rights, and the public interest.

These test environments will be able to prioritize the development of artificial intelligence systems aimed at solving social problems,



educational, financial inclusion, environmental sustainability, urban mobility, access to essential services, democratic strengthening and collective well-being.

The National Artificial Intelligence Council will actively participate in the design of testing environments and in the development of the National Roadmap for the Strategic Development of Artificial Intelligence, a planning tool that will establish priorities, principles, strategic sectors, and short-, medium-, and long-term objectives for the national artificial intelligence ecosystem.

The Council may also issue specific ethical guidelines and evaluation criteria, and require technical audits conducted by the National Algorithmic Audit Platform (PNAA) on the systems that are part of the testing environments.

Article 96. The main objective of a Regulatory Sandbox is to provide an environment that encourages innovation without compromising the principles of legality and protection of rights. These spaces allow for anticipating risks, detecting failures or biases at early stages, and better understanding the behavior of complex systems before their large-scale deployment. They also seek to strengthen collaboration between public institutions, universities, social organizations, and technology companies, with a view to building more precise and adaptive regulatory frameworks.

Article 97. Individuals or legal entities wishing to access a Test Environment must demonstrate that their project offers a technologically innovative proposal, with a potentially positive impact on society or strategic sectors.

They must submit an initial risk assessment, commit to transparency in the process, accept institutional oversight, and demonstrate that the system:

- I. Not be designed to perform actions prohibited by this Law;
- II. Nor generate, in its ordinary or foreseeable operation, responses, contents, instructions or decisions that involve activities



prohibited or of unacceptable risk under this Law.

III. They must also guarantee minimum conditions of traceability, explainability, and meaningful human oversight in automated decisions.

In applicable cases, interested parties may request a complementary technical evaluation from the National Algorithmic Audit Platform.

Article 98. Projects approved within a Test Environment will have an initial duration of up to twelve months, with the possibility of an additional extension, upon justification and justification.

During the trial period, the systems will undergo technical, ethical, and operational evaluations to identify both the benefits and limitations of the technology in question.

If at any time unacceptable risks are identified in accordance with the principles of this Law, the system may be immediately suspended by the competent authority.

If the results are positive, the system can move toward its formal authorization process, based on the corresponding risk level according to the Artificial Intelligence Risk Traffic Light.

The National Council for Artificial Intelligence may issue a temporary certification of technical and ethical validation, with the support of the National Algorithmic Audit Platform (PNAA), in cases where this is determined.

Article 99. Registration in a Test Environment will imply public registration of the project, which will include its general objective, the participating entities and the application sector.

During the testing phase, everyone interacting with the system must be clearly informed about its experimental nature and have the right to:



10. Be assisted by meaningful human supervision in any relevant interaction.

II. Challenge automated decisions that affect you, using accessible and timely mechanisms.

At the conclusion of the process, the results of the evaluations must be made public, except for information classified under applicable law.

For high-impact projects, a technical opinion issued by the National Algorithmic Audit Platform may be included as part of the public results file.

Article 100. Monitoring of Test Environments will be the responsibility of the competent authorities, who will have the technical support of the National Council of Artificial Intelligence and of academic institutions or independent research centers capable of guaranteeing an impartial, competent and ethical evaluation.

In cases where this is determined, the National Algorithmic Audit Platform may be integrated as a complementary technical body for the verification and evaluation of test projects.

CHAPTER XIX – PROMOTION OF RESEARCH, EDUCATION AND TALENT HUMAN

Article 101. The State, through its educational authorities, is responsible for progressively incorporating content into school curricula that addresses technological ethics, digital rights, and the logic of algorithms. This training must be adapted to each educational level and consider not only the development of technical skills but also the promotion of a critical approach to the use and effects of artificial intelligence on society. Linguistic and cultural inclusion in this content must be ensured, as well as a pedagogical perspective adapted to the country's diversity.



Article 102. The promotion of artificial intelligence in Mexico requires a solid foundation of human talent. To this end, the State will promote scholarship programs, alliances between universities, open laboratories in academic communities, and mechanisms that facilitate the return of Mexican professionals from abroad. The priority will be to train individuals capable of designing, implementing, and supervising Artificial Intelligence systems that respond to the country's social, economic, and environmental challenges.

Article 103. The construction of a national artificial intelligence ecosystem must be based on equity. Women, LGBTIQ+ people, indigenous communities, Afro-Mexicans, people with disabilities, and youth must have a guaranteed place in decision-making, technological creation, and research processes. Public policy must apply affirmative action when necessary and ensure that diversity is viewed as a structural value and not merely a quantitative goal.

Article 104. All scientific initiatives developed with public resources must be documented, registered, and, to the extent possible, made available to the public in open formats. The authorities will promote the creation of a National Registry of AI Projects, where advances, findings, and relevant tools will be published, always protecting confidential or sensitive information. Likewise, public recognition will be encouraged for research that stands out for its social value, ethical soundness, or usefulness in addressing national challenges.

Article 105. In order to guarantee the human right to science and the public interest, information generated from research and technological development activities in the field of artificial intelligence that are financed, promoted, or supported by the State must be openly accessible, except in cases where applicable legislation establishes restrictions for reasons of intellectual property, national security, protection of personal data, or other legal provisions.

Article 106. The competent authorities, in coordination with academic institutions, social organizations, cooperatives and others



Relevant actors will promote technological training programs for the development of skills in artificial intelligence and emerging technologies, primarily aimed at vulnerable communities.

Linguistic, cultural, and territorial inclusion will be guaranteed, respecting the rights of indigenous peoples to receive training in their native language and under culturally appropriate conditions.

Article 107. Any Artificial Intelligence system used in automated learning processes, digital certification, or performance evaluation must guarantee transparency of criteria, interoperability with national education systems, and enhanced protection of school data.

CHAPTER XX — INTERNATIONAL COOPERATION AND MULTILATERALISM TECHNOLOGY IN ARTIFICIAL INTELLIGENCE

Article 108. The Mexican State will actively promote international cooperation in the development, regulation, supervision, and use of artificial intelligence, based on respect for human rights, human dignity, peace, sustainable development, and the technological self-determination of peoples.

Article 109. Mexico will participate in forums, initiatives, and multilateral organizations that promote the ethical and transparent governance of artificial intelligence, encouraging the exchange of good practices, the development of global standards, and international regulatory harmonization regarding digital rights, personal data protection, algorithmic explainability, and technological oversight.

Article 110. The State will promote international cooperation programs that promote the responsible transfer of knowledge, technologies and capabilities in the field of artificial intelligence, especially towards developing countries, respecting sovereignty, technological and the principle of international equity.

Article 111. The implementation of the actions derived from this chapter will correspond to the competent authorities, in coordination



with the Ministry of Foreign Affairs, the Ministry of Economy, the National Council for the Humanities, Science, Technology and Innovation, and other relevant bodies, in accordance with their respective powers.

CHAPTER XXI – SUSTAINABILITY AND ENVIRONMENTAL IMPACT

Article 112. The planning, development, implementation, and use of artificial intelligence must be carried out under criteria of energy efficiency, technological circularity, and environmental protection, reducing its ecological footprint and contributing to national and international climate and sustainable development objectives. Likewise, every artificial intelligence strategy or project must verify its alignment with the **Sustainable Development Goals (SDGs)** of the 2030 Agenda, ensuring its effective contribution to the objectives of sustainability, equity, and resilience.

Additionally, at the urban and territorial levels, adherence to the principles established in the **International Guidelines for the Development of People-Centered Smart Cities should be promoted**, ensuring that technological integration strengthens the right to the city, social inclusion, and environmental sustainability.

Article 113. Environmental assessment of high consumption systems

Any artificial intelligence system that requires intensive data processing, massive model training, or operates on energy-intensive infrastructure must undergo a Technological Environmental Impact Assessment (TEIA).

This assessment should consider:

- I. Estimated energy and water consumption.
- II. The energy source used (renewable or not).
- III. Indirect carbon emissions from the system.



IV. The use of critical materials, strategic minerals or resources scarce.

V. The destination of electronic components at the end of their useful life.

The competent authority may establish maximum consumption limits, require mitigation measures, or condition the authorization of the system based on its ecological footprint.

Article 114. Requirements for data centers and processing

Data centers, private clouds, or technological infrastructure that operates artificial intelligence systems must:

I. Optimize your energy efficiency.

II. Prioritize the use of clean energy.

III. Have sustainable cooling systems.

IV. Implement progressive emissions reduction plans.

V. Publish annual operational sustainability reports.

The authority may require environmental certification of these infrastructures as a condition for their operation in strategic sectors.

Article 115. The State will promote the development of Sustainable Artificial Intelligence, understood as that which is oriented towards:

I. Improve the energy efficiency of industrial, logistics and processes urban.

II. Optimize the management of waste, water and natural resources.



III. Monitor ecosystems, biodiversity, climate change and environmental phenomena.

IV. Reduce the carbon footprint in transportation, production or consumption.

V. Prevent natural disasters and protect protected natural areas.

Article 116. National and international individuals or legal entities that develop, manufacture, import or dispose of components used in Artificial Intelligence (chips, sensors, servers, connected equipment) must:

I. Comply with the provisions of the General Law for the Prevention and Comprehensive Waste Management.

II. Establish plans for recycling, collection and safe disposal of electronic waste.

III. Prioritize the use of recyclable, biodegradable, or low-impact materials.

IV. Avoid practices that transfer negative environmental impacts to vulnerable communities or marginalized territories.

Article 117. The State may grant fiscal, financial or regulatory incentives to Artificial Intelligence projects that:

VO. Use certified sustainable infrastructure.

II. Demonstrate verifiable reduction in environmental impact.

III. Be aligned with the 2030 Agenda, the International Guidelines for the Development of People-Centered Smart Cities, the Paris Agreement, and the National Climate Change Strategy.



IV. Be developed by communities, cooperatives, or social actors committed to climate justice.

CHAPTER XXII – OWNERSHIP AND COPYRIGHT IN ENVIRONMENTS AUTOMATED

Article 118. It is recognized that artificial intelligence systems can generate literary, artistic, musical, visual, scientific or technical works, the originality of which may derive from human creative intervention, automated processes or a combination of both.

Article 119. The ownership of property rights over a work generated by artificial intelligence shall be determined based on the degree of significant human intervention. The author shall be understood to be the natural or legal person who:

1. Provided instructions, creative context, or supervision substantial to the automated process.
2. Be the owner of the Artificial Intelligence system and have developed the model for explicit creative purposes.
3. Has generated the work directly through meaningful human interaction with the AI.

In the absence of verifiable creative human intervention, the work may be considered not eligible for copyright protection, unless otherwise provided.

Article 120. In cases where there is no significant human intervention, the generating system cannot be considered the legal author.

The work may be incorporated into the public domain or subject to a regime in accordance with the provisions of regulatory legislation.



CHAPTER XXIII – USE OF PROTECTED DATA FOR TRAINING AI SYSTEMS

Article 121. The use of copyrighted works as part of a data set for training Artificial Intelligence models will require:

- I. Express consent of the rights holder, when this
are affected by inappropriate use.
- II. Valid licensing or usage agreements in accordance with the law.
- III. Exceptions provided for in national and international legal frameworks
international, duly justified.

Article 122. In those cases where the result produced by the system may constitute an infringement under current copyright legislation, due to the partial or total reproduction of a work, mechanisms must be implemented for its detection, prevention and, where appropriate, remediation in accordance with the law.

Article 123. Every developer of Artificial Intelligence systems must:

- I. Document the origin and licensing of data sets
employees.
- II. Establish traceability mechanisms for content used in the
training.
- III. Publish an accessible summary of the sources used, except for information classified for
security or privacy reasons.
- IV. Enable a section on its official website clearly identified as Algorithmic Training Information, in
which clear, structured, and understandable information on the methods, sources, criteria,
and processes used in training the AI system must be made available to the general public.



CHAPTER XXIV – EXCLUSIVE USE OF REGISTERED TRADEMARKS IN SYSTEMS

FROM AI

Article 124. The use of registered trademarks in artificial intelligence systems shall be exclusively reserved for the trademark owner and the natural or legal persons expressly authorized by the owner in writing. This right includes the generation of images, text, video, audio, or other visual or symbolic representations related to the trademark, using automated technologies.

Article 125. The unauthorized use of registered trademarks in content generated by artificial intelligence systems, including those simulating packaging, logos, products, or associated visual elements, will be considered an infringement of industrial property rights, with potential penalties for reputational damage, consumer confusion, or misleading use of a commercial identity.

CHAPTER XXV – ADAPTATION OF LEGAL FRAMEWORKS AND STIMULUS TO CREATIVE INNOVATION

Article 126. Review of regulatory frameworks.

The competent authority, in coordination with the National Institute of Copyright (INDAUTOR) will propose reforms to the Federal Law of Copyright and other applicable laws for:

- I. Recognize new models of hybrid human-AI creation.
- II. Establish specific mechanisms for registering generated works by AI.
- III. Protect the rights of human creators against automated use of their works.



Article 127. The State shall promote the development and adoption of artificial intelligence models compatible with respect for copyright, through:

I. Voluntary certification programs for responsible developers.

II. Public recognition of good practices in AI-assisted creativity.

III. Preferential access to public financing for ethical projects of creative Artificial Intelligence.

CHAPTER XXVI – SUPERVISION AND INSPECTION

Article 128. The competent authorities, in accordance with the provisions of this Law, may:

I. Request technical, legal or administrative information from developers, operators or institutional users of AI systems.

II. Conduct audits, verifications or inspections in the field or digital.

III. Access, by means of a reasoned order, to operating records, traceability or databases of the systems.

IV. Order the temporary or permanent suspension of systems that violate legal provisions, cause harm, or pose unacceptable risks.

V. Collaborate with international authorities to oversee cross-border or global systems.

Article 129. The National Council for Artificial Intelligence will coordinate with other authorities the implementation of mechanisms for:

I. Periodic evaluation of compliance with this Law.



- II. Supervision of high-risk systems and strategic sectors.
- III. Publication of compliance reports, with indicators verifiable.
- IV. Coordination with internal and external control bodies in public entities.
- V. Strengthening supervisory capacities in regulatory bodies.

Article 130. Artificial Intelligence systems classified as high risk must be audited:

- I. Techniques, on operation, precision, failures and efficiency.
- II. Legal, on compatibility with fundamental rights, data protection, equity and proportionality.
- III. Ethics, biases, unintended impacts and social effects.

These audits may be carried out by accredited entities, public universities, research centers, or independent specialized auditors.

CHAPTER XXVII – SYSTEM OF INFRACTIONS AND PENALTIES

Article 131. The following constitute violations of this Law:

- I. Implement Artificial Intelligence systems without meeting classification, registration or impact assessment requirements.
- II. Hiding or falsifying information during audit or investigation processes supervision.
- III. Develop or use prohibited systems or systems that cause non-human harm. reported.
- IV. Failure to guarantee appeal mechanisms, human oversight, or traceability.



V. Failure to comply with obligations regarding child protection, strategic sectors or the environment.

VI. Repeat technical failures that affect fundamental rights.

Article 132. Violations of the provisions of this Law will result in the imposition of one or more of the following sanctions:

VO. Public reprimand.

II. Temporary suspension of the system, project or service.

III. Cancellation of registration or revocation of operating authorization in the National Registry of Artificial Intelligence Systems (RENSIA).

IV. Imposition of fines according to the following scheme:

a. Minor infractions: from 50 to 500 Measurement Units and Update (UMA).

b. Serious violations: from 501 to 100,000 UMA.

c. Very serious violations: exceeding 100,000 UMA.

The seriousness of the violation will be determined by considering factors such as repeat offenses, the level of impact on human rights, the magnitude of the social or economic harm, the number of people affected, and the degree of intentionality or negligence.

V. Temporary disqualification, from one to five years, from participating in public procurement procedures related to artificial intelligence technologies.

VI. Obligation to repair individual or collective damage caused, through measures of restitution, compensation, satisfaction,



rehabilitation or guarantees of non-repetition, in accordance with applicable legislation.

Sanctions will be imposed through administrative proceedings, guaranteeing the persons or entities allegedly responsible the right to a hearing, adequate defense, and access to administrative or judicial review mechanisms.

Article 133. When using an artificial intelligence system:

- I. Causes injury, death, deprivation of liberty, serious property damage, or
- II. Be part of criminal conduct such as fraud, electoral manipulation, digital violence, human trafficking or illegal surveillance,

The facts may be prosecuted criminally in accordance with the Federal Penal Code, without prejudice to administrative or civil sanctions.

Article 134. To determine the specific amount of the sanction within the established range, the competent authority must assess the following elements in a reasoned and reasoned manner:

- I. The nature and severity of the damage caused;
- II. The level of risk associated with the system involved;
- III. The number of people affected and their vulnerability;
- IV. The existence or not of intentionality, fraud or negligence;
- V. Recurrence of similar behavior;
- VI. The economic benefit obtained from the infringement;
- VII. The degree of cooperation with the investigation or repair of the damage.

Article 135. The sanctions provided for in this Law shall be imposed by the competent authorities in accordance with their legal and regulatory powers, in accordance with the nature of the violation, the sector involved, and the type of impact generated.



The National Council for Artificial Intelligence and the National Algorithmic Audit Platform may issue opinions, alerts, technical reports, or audits that serve as evidence or technical references in the corresponding administrative, civil, or criminal proceedings.

Sanctioning authorities must guarantee due process, the right to defense, and the proportionality of the sanctions imposed, in accordance with applicable law.

CHAPTER XXVIII – COMPLAINT, REVIEW AND REMEDY MECHANISMS OF THE DAMAGE

Article 136. Every person shall have the right to file individual or collective complaints when they consider that they have been directly or indirectly affected by the improper, unfair, discriminatory, opaque, or dangerous use of an artificial intelligence system.

Complaints may be filed digitally, in writing, or in person to:

- I. The competent authorities in matters of data protection, human rights, consumers, children or cybersecurity.
- II. The National Council for Artificial Intelligence.
- III. Platforms or entities operating the reported system, who must have accessible channels and internal procedures.

Article 137. The reporting mechanisms must:

- I. Be free, accessible, secure, and provide whistleblower protection.
- II. Allow anonymous or confidential complaints, when appropriate.
justify.
- III. Generate acknowledgment of receipt and file or folio number.
- IV. Allow digital monitoring of the process status.



V. Establish reasonable deadlines for issuing a response.

VI. Activate precautionary measures if there is imminent risk to rights humans.

Article 138. Persons affected by a decision made by an Artificial Intelligence system may request:

I. Its review by a competent authority or human person.

II. The technical and legal explanation of the process followed.

III. The temporary suspension of its effects while the claim is resolved.

IV. Rectification, reversal or compensation of damage when proceed.

The operating entities must respond within 15 business days. If there is no response, the individual may appeal to the administrative or judicial authorities.

Article 139. The State shall guarantee access to:

I. Public defenders specialized in digital rights, algorithms and technologies.

II. Autonomous human rights protection bodies with the power to investigate and issue recommendations.

III. Social and academic organizations with experience in algorithmic justice, digital ethics, or technological vulnerability.

IV. Administrative authorities may request technical support from the PNAA to analyze the algorithmic architecture and determine whether there was an error, bias, or design flaw.

V. The support will be free, prioritized for people in vulnerable situations, and will offer an intercultural focus.



Article 140. When a person is affected by decisions, omissions, biases, errors or negligence in the use of AI, they shall have the right to full reparation, which may include:

- I. Restoration of violated rights.
- II. Financial compensation for damages.
- III. Psychological or community rehabilitation, if applicable.
- IV. Guarantees of non-repetition, such as structural adjustments to the system.
- V. Public recognition of the damage and symbolic measures of repair.

Administrative, judicial, or regulatory authorities may order these remedies depending on the severity of the case and the applicable legal framework.

CHAPTER XXIX. FINAL AND TRANSITIONAL PROVISIONS

Article 141. The competent authorities shall promote the harmonization of this Law with other general and federal laws on personal data protection, science and technology, cybersecurity, transparency, digital justice, the rights of children and adolescents, and consumer protection, without prejudice to the powers of local Congresses.

Article 142. In matters not provided for by this Law, the Political Constitution of the United Mexican States, international treaties on human rights, and the provisions of general and federal laws applicable in this matter shall apply on a supplementary basis.

Article 143. The Federal Executive, the federated entities and the municipalities, within the scope of their powers, must issue or adapt the regulations, technical standards, guidelines and other provisions necessary for the correct implementation of this Law.

Article 144. The National Council for Artificial Intelligence must propose to the Congress of the Union, every three years, a report with proposals for legislative updates and recommendations for improving the framework.



regulatory based on technological advances and emerging challenges in the field.

Article 145. Any interpretation of this Law must be made in accordance with the pro-persona principle, always prioritizing the broadest protection of human rights recognized in the Constitution and in the international treaties to which the Mexican State is a party.

TRANSIENTS

First. This Law will enter into force 90 calendar days following its publication in the Official Gazette of the Federation.

Second. The Federal Executive, through the competent agencies, must issue the Regulations for this Law within 180 calendar days of its entry into force.

Third. The authorities provided for in Article 7 of this Law must, within 120 calendar days of its entry into force, form the National Council on Artificial Intelligence, in accordance with the provisions of Chapter II. Every three years, the National Council on Artificial Intelligence must submit to the Congress of the Union a report with proposals for legislative updates and recommendations for improving the regulatory framework based on technological advances and emerging challenges in this area.

Fourth. The National Registry of Artificial Intelligence Systems (RENSIA) must begin operations within 240 calendar days following the publication of the Regulations of this Law. Public and private entities operating high-risk systems must register within a period of no more than 180 calendar days following the start of RENSIA operations.

Fifth. Public entities must establish internal algorithmic ethics committees and accountability mechanisms within a period of no more than nine months after the Regulation comes into force.



Sixth. The Ministry of Public Education, in coordination with the Ministry of Science, Humanities, Technology, and Innovation, must implement a national artificial intelligence literacy program within a period of no more than 12 months from the date the Regulations come into force.

Seventh. Artificial intelligence systems classified as prohibited under this Law must be deactivated within a period of no more than 30 calendar days from the publication of their official classification, and noncompliance will be sanctioned in accordance with applicable provisions.

Eighth. The National Council on Artificial Intelligence must issue the technical and operational guidelines for the installation, operation, and evaluation of the National Algorithmic Audit Platform within a period of no more than 180 days from the date this decree enters into force.

Ninth. The competent authorities shall promote the harmonization of this Law with other general and federal laws on personal data protection, science and technology, cybersecurity, transparency, digital justice, national security, the rights of children and adolescents, and consumer protection, without prejudice to the powers of local Congresses, within 160 business days.

In matters not covered by this Law, the Political Constitution of the United Mexican States, international treaties on human rights, and the provisions of general and federal laws applicable to the matter shall apply on a supplementary basis.



Declaro que los procedimientos de investigación o juicios relacionados con los derechos humanos causados por la aplicación de la ley de esta Ley no serán considerados como resoluciones firmes.

Legislative Assembly of San José, April 22, 2025

Dip. Gabriela Georgina Jiménez
Gabby

Dip. Sergio Carlos Gutiérrez Luna

Dip. Beatriz Legom. Perez Cruz

Dip. Ávila Villegas Braniel

Dip. Flores Cervantes Hugo Eric

Dip. Herrera Berunda Javier Octavio

Dip. Ramírez Cuéllar Alfonso

Dip. Alvarez Flaner

Dip. Carvajal Hidalgo Alejandro

Dip. Mayer Bretón Sergio

Dip. Arellano Ávila Giselle Yunueen

Dip. Zeballos Alvarado Joaquín

Dip. Harbo de J. Espino

Dip. Gndy Canat

Dip. 0/9a/Fanaa asdw



DIP. JUAN ANGELO FLORES BU FAMANTE

[Signature]

Dip. Santiago Rodríguez Guillermo
Rafael Armando

[Signature]
Maya

Dip. Fernández Samaniego José
Armando

[Signature]

Dip. Flores Ojeda Doris
Margarita

[Signature]

Dip. Herrera Villavicencio Mónica

[Signature]

Dip. Fernández Cesa Mónica

[Signature]

Dip. Herrera Ramos Jesús Alfonso

[Signature]
H Ser

Dip. Gilberto Herrera Solís

[Signature]
Representative Govila Sanchez Lopez

Solís Dip. Claudia Garza Hder
Olaike

[Signature]
Harisda Lunigal
Sow

Dip Lise Mos Hao

[Signature]
Id

Dp Eder Gaca Medine

[Signature]
DIRXV MenE

Alma Laura Rutz 1gez h

58
[Signature]
Julieta Varas Valencio

Chamber of Deputies of the Honorable Congress of the Union, LXVI Legislature

Political Coordination Board

Deputies: Ricardo Monreal Ávila, president; José Elias Lixa Abimerhi, National Action Party (PAN); Carlos Alberto Puente Salas, PVEM; Reginaldo Sandoval Flores, PT; Rubén Ignacio Moreira Valdez, PRI; Ivonne Aracely Ortega Pacheco, CITIZEN MOVEMENT .

Board of Directors

Deputies: Sergio Carlos Gutiérrez Luna, president; vice presidents: María de Dolores Padierna Luna, MORENA; Kenia López Rabadán, PAN; María Luisa Mendoza Mondragón, PVEM; secretaries: Julieta Villalpando Riquelme, MORE-NA; Alan Sahir Márquez Becerra, PAN; Nayeli Arlen Fernández Cruz, PVEM; José Luis Montalvo Luna, PT; Fuensanta Guadalupe Guerrero Esquivel, PRI; Laura Iraís Ballesteros Mancilla, CITIZEN MOVEMENT .

General Secretariat

Secretariat of Parliamentary Services

Parliamentary Gazette of the Chamber of Deputies

Director: Juan Luis Concheiro Bórquez, Editing: Casimiro Femat Saldívar, Ricardo Águila Sánchez, Antonio Mariscal Pioquinto.

Documentary Support: General Directorate of Legislative Process. Address: Avenida Congreso de la Unión, number 66, building E, fourth floor, Legislative Palace of San Lázaro, colonia El Parque, CP 15969. Telephone: 5036 0000, extension 54046. Electronic address: <http://gaceta.diputados.gob.mx/>